IN THE CLAIMS:

Please cancel claims 24-26, and amend the claims as follows:

1. (Previously Presented): A method for processing a fragmented packet with a firewalling device, comprising:

receiving fragments of the packet prior to processing of firewall policies at the firewalling device;

sorting the fragments according to the packet and order of the fragments;

storing the fragments in association with the packet and in order in a connection table (CT) and a Network Address Translation table (NT);

cross linking the NT and CT by storing a hash of at least a portion of the fragments in one of the NT and CT tables;

collecting and assembling all the fragments in order to fully reconstitute the packet prior to applying firewall policies;

storing an Address Research Table (ART) for a first packet of a connection to the firewall device in association with one of the NT and the CT, and the hashing each of the subsequent packets to determine a table entry to forward the packet; and

transferring the packet to the firewalling device to apply the firewall policies to the entire packet at one time.

2. (Previously Presented): The method, according to claim 1, further comprising:

obtaining source and destination address information for the fragments; and

determining if the source and destination address information of the fragments matches of the other fragments.

3. (Original): The method, according to claim 1, further comprising determining if the fragments have a valid checksum.

4. (Original): The method, according to claim 1, wherein the sorting comprises obtaining packet and fragment identifiers.

5. (Original): The method, according to claim 4, further comprising determining if any of the fragments needed to reconstitute the packet have not been stored.

6. (Original): The method, according to claim 5, further comprising determining if the fragments stored collectively exceed a communication length threshold.

7. (Original): The method, according to claim 6, further comprising purging the fragments responsive to the communication length threshold being exceeded.

8. (Original): The method, according to claim 7, further comprising starting a timer in association with an initial one of the fragments received by the firewalling device.

9. (Original): The method, according to claim 8, further comprising checking whether all the fragments needed to reconstitute the packet have not been received to the firewalling device within a threshold time period.

10. (Original): The method, according to claim 1, wherein the storing comprises overwriting one of the fragments with a subsequently received fragment.

11. – 28. (Cancelled)

29. (Previously Presented): The method of claim 1, including comparing information from each received packet to the previous received packet before forwarding the packet.

30. (Previously Presented): The method of claim 1, wherein the hash function is based on the incoming packet 5-triple information.

31. (Previously Presented): The method of claim 30, wherein the input to the hash function of the NT index uses public address information.

32. (New): A computer readable medium containing instructions that, when executed by a processor, cause the processor to process a fragmented packet with a firewalling device, by performing the steps of:

receiving fragments of the packet prior to processing of firewall policies at the firewalling device;

sorting the fragments according to the packet and order of the fragments;

storing the fragments in association with the packet and in order in a connection table (CT) and a Network Address Translation table (NT);

cross linking the NT and CT by storing a hash of at least a portion of the fragments in one of the NT and CT tables;

collecting and assembling all the fragments in order to fully reconstitute the packet prior to applying firewall policies;

storing an Address Research Table (ART) for a first packet of a connection to the firewall device in association with one of the NT and the CT, and the hashing each of the subsequent packets to determine a table entry to forward the packet; and

transferring the packet to the firewalling device to apply the firewall policies to the entire packet at one time.

33. (New): The computer readable medium, according to claim 32, further comprising:

obtaining source and destination address information for the fragments; and

determining if the source and destination address information of the fragments matches of the other fragments.

34. (New): The computer readable medium, according to claim 32, further comprising determining if the fragments have a valid checksum.

35. (New): The computer readable medium, according to claim 32, wherein the sorting comprises obtaining packet and fragment identifiers.

36. (New): The computer readable medium, according to claim 32, further comprising determining if any of the fragments needed to reconstitute the packet have not been stored.

37. (New): The computer readable medium, according to claim 36, further comprising determining if the fragments stored collectively exceed a communication length threshold.

38. (New): The computer readable medium, according to claim 37, further comprising purging the fragments responsive to the communication length threshold being exceeded.

39. (New): The computer readable medium, according to claim 38, further comprising starting a timer in association with an initial one of the fragments received by the firewalling device.

40. (New): The computer readable medium, according to claim 39, further comprising checking whether all the fragments needed to reconstitute the packet have not been received to the firewalling device within a threshold time period.

41. (New): The computer readable medium, according to claim 32, wherein the storing comprises overwriting one of the fragments with a subsequently received fragment.